United Nations A/CN.9/604

General Assembly

Distr.: General
9 May 2006

Original: English

United Nations Commission on International Trade Law
Thirty-ninth session
New York, 19 June-7 July 2006

Possible future work in the area of electronic commerce

Note by the Secretariat*

Contents

		Paragraphs	Page
I.	Introduction	1-6	3
II.	Possible topics for a comprehensive reference document in the area of electronic commerce	7-62	4
	A. Authentication and cross-border recognition of electronic signatures	7-17	4
	1. The issues	7-13	4
	2. Justification and proposed approach	14-17	6
	B. Liability and standards of conduct for information service providers	18-24	7
	1. The issues	18-21	7
	2. Justification and proposed approach	22-24	7
	C. Electronic invoicing and legal issues related to supply chains in electronic commerce	25-31	8
	1. The issues	25-28	8
	2. Justification and proposed approach	29-31	9

* Submission of this document was delayed due to late receipt of contributions by outside experts.

V.06-53896 (E) 290506 290506

D. Transfer of rights in tangible goods and other rights through electronic communications 32-41 10

1. The issues 32-38 10

2. Justification and proposed approach 39-41 12

E. Unfair competition and deceptive trade practices in electronic commerce 42-46 12

1. The issues 42-43 12

2. Justification and proposed approach 44-46 13

F. Privacy and data protection in electronic commerce 47-52 14

1. The issues 47-49 14

2. Justification 50-52 14

G. Other elements for a sound legal framework for electronic commerce 53-62 15

1. Protection of intellectual property rights 53-57 15

2. Consumer protection in electronic commerce 58-60 16

3. Unsolicited electronic communications (spam) 61 17

4. Cybercrime 62 17

III. Proposed nature of future work 63-65 17

I. Introduction

1. At its thirty-eighth session, the Commission considered the possibility of undertaking future work in the area of electronic commerce in the light of a note submitted by the Secretariat in pursuance of the Commission's mandate to coordinate international legal harmonization efforts in the area of international trade law.[1] In that note, the Secretariat had summarized the work undertaken by other organizations in various areas related to electronic commerce (A/CN.9/579). It was pointed out that the range of issues currently being dealt with by various organizations were indicative of the various elements required to establish a favourable legal framework for electronic commerce.

2. It was then pointed out that the UNCITRAL Model Law on Electronic Commerce,[2] the UNCITRAL Model Law on Electronic Signatures,[3] as well as the Convention on the Use of Electronic Communications in International Contracts,[4] which the Commission approved during that session, provided a good basis for States to facilitate electronic commerce, but only addressed a limited number of issues. The Secretariat noted that more needed to be done to enhance confidence and trust in electronic commerce, such as appropriate rules on consumer and privacy protection, cross-border recognition of electronic signatures and authentication methods, measures to combat computer crime and cybercrime, network security and critical infrastructure for electronic commerce and protection of intellectual property rights in connection with electronic commerce, among various other aspects. It was further noted that there was no single international document providing guidance to which legislators and policymakers around the world could refer for advice on those various aspects. The task of legislators and policymakers, in particular in developing countries, might be greatly facilitated if such a comprehensive reference document were to be formulated.[5]

3. The Commission welcomed the information provided in the note by the Secretariat and confirmed the usefulness of such cross-sectoral overview of activities from the viewpoint both of its coordination activities and of the information requirements of Member States. There was general agreement that it would be useful for the Secretariat to prepare a more detailed study, in cooperation and in consultation with the other international organizations concerned, for consideration by the Commission at its thirty-ninth session, in 2006. Such an overview, with proposals as to the form and nature of the reference document that would be envisaged, would be useful to allow the Commission to consider possible areas in which it could itself undertake legislative work in the future, as well as areas in which legislators and policymakers might benefit from comprehensive information, which did not necessarily need to take the form of specific legislative guidance. It was agreed that, in considering that matter, the Commission should bear in mind the need to ensure appropriate coordination and consultation with other organizations and to avoid duplicating or overlapping work.[6]

4. As regards the range of issues to be considered in such a detailed overview, the following areas were suggested: transfer of rights in tangible goods or other rights through electronic communications, intellectual property rights, information security, cross-border recognition of electronic signatures, electronic invoicing and online dispute resolution. The Commission's attention was also drawn to the recommendations for future work that had been made by the Working Group (see

A/CN.9/571, para. 12). It was agreed that those recommendations should also be considered in the context of the detailed overview to be prepared by the Secretariat, to the extent that some of them were not reflected in the explanatory notes to the Convention on the Use of Electronic Communications in International Contracts, which the Secretariat has prepared pursuant to the Commission's request (see A/CN.9/608 and Addenda 1-4), or in separate information activities undertaken by the Secretariat, such as monitoring the implementation of the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures, and compiling judicial decisions on the matters dealt with in those Model Laws.[7]

5. The present note is submitted pursuant to the Commission's request. It identifies the issues proposed to be considered for inclusion in a comprehensive reference document. This note explains the relationship between the various issues and the Commission's area of work and offers suggestions on possible ways of dealing with them.

6. This note should be read in conjunction with the note A/CN.9/579, on current work by other organizations in the area of electronic commerce, which was submitted to the Commission's thirty-eighth session, and note A/CN.9/598, paragraphs 15 to 34, of the current session, which contains update information on the same matter. With a view to avoiding repetition, and in compliance with the General Assembly guidelines on limitation of documentation, this note omits references already contained in those two notes.

II. Possible topics for a comprehensive reference document in the area of electronic commerce

A. Authentication and cross-border recognition of electronic signatures

1. The issues

7. In an electronic environment, the original of a message is indistinguishable from a copy, bears no handwritten signature, and is not on paper. This may give rise to fears about possible misuse or fraud due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions. The purpose of various techniques currently available on the market or still under development is to offer technical means by which some or all of the functions identified as characteristic of handwritten signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures".

8. One such technique makes use of pairs of mathematically related "keys" (i.e. large numbers produced using a series of mathematical formulae) to generate an electronic signature (called "digital signature"), and verify that it originates from the purported signatory. One of the keys (the "private key" kept secret by the signatory) is used for creating a digital signature or transforming data into a seemingly unintelligible form, while the other one (the "public key" made known to the addressee) is used for verifying a digital signature or returning the message to its original form. However, since a public- and private-key pair has no intrinsic

association with any person, the addressee needs additional assurance about the usefulness of the public key to identify the signatory. One type of solution to this problem is the use of one or more third parties to associate an identified signatory or the signatory's name with a specific public key. These third parties are generally referred to as a "certification service providers", and in a number of countries their functions are being organized hierarchically into what is often referred to as a "public-key infrastructure" (PKI). However, other solutions may include, for example, certificates issued by relying parties.

9. In practice, suppliers of certification services issue certificates with various levels of reliability, according to the purposes for which the certificates are intended to be used by their customers. Depending on their respective level of reliability, certificates and electronic signatures may produce varying legal effects, both domestically and abroad. For example, in certain countries, even certificates that are sometimes referred to as "low-level" or "low-value" certificates might, in certain circumstances (e.g. where parties have agreed contractually to use such instruments), produce legal effect.

10. Legal issues may arise with regard to cross-certifying or chaining of certificates when there are multiple security policies involved. Examples of such issues may include determining whose misconduct caused a loss and upon whose representations the user relied. These matters are often dealt with at a contractual level; through certification practices statements and general conditions of contract of certification service providers. With a view to promoting the development of an industry still in its infancy, and to protect it against potentially threatening exposure to claims for consequential damages, some jurisdictions admit limitations or exclusions of liability, where the levels of security and policies are made known to the users and there is no negligence on the part of certification authorities. However, the extent to which certification service providers may disclaim liability for loss or damage caused by service failure, or may limit their liability in those cases, is likely to vary from country to country.

11. Alongside "digital signatures" based on public-key cryptography, there exist various other devices, also covered in the broader notion of "electronic signature" mechanisms, which may currently be used, or considered for future use, with a view to fulfilling one or more of the above-mentioned functions of handwritten signatures. For example, certain techniques would rely on authentication through a biometric device based on handwritten signatures. In such a device, the signatory would sign manually, using a special pen, either on a computer screen or on a digital pad. The handwritten signature would then be analysed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the relying party for authentication purposes. Such an authentication system would presuppose that samples of the handwritten signature have been previously analysed and stored by the biometric device. Other techniques would involve the use of personal identification numbers (PINs), digitized versions of handwritten signatures, and other methods, such as clicking an "OK-box".

12. Article 12 of the UNCITRAL Model Law on Electronic Signatures encourages States to promote cross-border recognition of electronic signatures. Paragraph 1 of that article reflects the basic principle that the determination of whether and to what extent a certificate or an electronic signature is capable of being legally effective should not depend on the place where the certificate or the electronic signature was

issued but on its technical reliability. Paragraph 2 of that article provides the general criterion for the cross-border recognition of certificates without which suppliers of certification services might face the unreasonable burden of having to obtain licences in multiple jurisdictions. The threshold for technical equivalence of foreign certificates is based on testing their reliability against the reliability requirements established by the enacting State pursuant to the Model Law, regardless of the nature of the certification scheme obtaining in the jurisdiction from which the certificate or signature originates.

13. Article 12, paragraphs 2 and 3, of the Model Law on Electronic Signatures deal exclusively with the cross-border reliability test to be applied when assessing the reliability of a foreign certificate or electronic signature. However, in the preparation of the Model Law, it was borne in mind that enacting States might wish to obviate the need for a reliability test in respect of specific signatures or certificates, when the enacting State was satisfied that the law of the jurisdiction from which the signature or the certificate originated provided an adequate standard of reliability. As to the legal techniques through which advance recognition of the reliability of certificates and signatures complying with the law of a foreign country might be made by an enacting State (e.g. a unilateral declaration or a treaty), the Model Law contains no specific suggestion.

2. Justification and proposed approach

14. The lack of common standards for cross-border recognition of electronic signatures and other authentication methods is considered to be a significant impediment to cross-border commercial transactions. Two main problems exist in the given context. On the one hand, technological measures and systems for electronic signatures, in particular digital signatures, are currently much too diverse to enable uniform international standards. On the other hand, fears about fraud and manipulation in electronic communications have led some jurisdictions to establish rather stringent regulatory requirements, which in turn may have discouraged the use of electronic signatures, in particular digital signatures.

15. Wide accession to the recently adopted United Nations Convention on the Use of Electronic Communications in International Contracts, which provides in its article 9 for the functional equivalence between electronic signatures and traditional types of signature, may go a long way towards facilitating cross-border use of electronic signatures. Nevertheless, notarization of electronic documents and electronic signatures in government or other official records are areas in which governments may be inclined to retain national standards capable of hindering or barring recognition of foreign electronic signatures.

16. The issues described above have been under consideration by a number of international organizations, including OECD (see A/CN.9/579, paras. 43-46; A/CN.9/598, paras. 27-28); the European Union (A/CN.9/579, para. 34; A/CN.9/598, para. 21); APEC (A/CN.9/579, paras. 22-26; A/CN.9/598, para. 17), and the Commonwealth secretariat (A/CN.9/598, para. 20). Not all organizations deal with every aspect of these issues and the perspective from which each organization discusses them is not necessarily identical. This variety of sources and diversity of approaches does not facilitate the task of legislators and policymakers interested in establishing a sound legal framework for interoperability and cross-border use of electronic signatures.

17. The Commission may wish to consider that it would be useful to include the issues of authentication and cross-border recognition of electronic signatures in a comprehensive reference document.

B. Liability and standards of conduct for information service providers

1. The issues

18. Information service providers play an essential role in the functioning of the Internet. Typically, they act as intermediaries who transmit or host third party content but do not take part in the decision to disseminate particular material. Liability may arise from theories of direct and indirect or contributory infringement in national tort law, criminal law, and intellectual property law. Most cases arise from the fact that service providers take part in the technical process of transmitting or storing information for third party content of any kind.

19. Responsibility for unlawful content or unlawful acts of their users is related to the opportunity and extent of control that information service providers are able to exert. The possibilities of storage and transmission of data files in data networks have multiplied the opportunities of unlawful behaviour and reduced chances of detection and control. Hence, imposing general liability for service providers would amount to establishing duties to monitor and filter all transmitted or stored content—a burdensome task for information service providers for technical and economic reasons as well as unacceptable for other reasons. As a result, many countries have perceived a need for limiting liability of information services.

20. However, the interest in limiting liability of service providers has to be weighed against the interests of rightholders and injured parties in enforcing their rights and holding all contributing parties responsible. It does not seem to be necessary that the approaches be identical: they may differ depending on the particular circumstances and legal traditions in any given country. But they should be interoperable if global networks and electronic commerce are to develop smoothly.

21. An additional set of legal issues relates to the possible liability of information service providers for failures that occur during transmission of messages (delivery delay or loss of information), or for malfunctioning of data storage systems (loss of stored data or unauthorized access by third parties). Typically, these matters would be dealt with at a contractual level, through general conditions of contract of information service providers. However, the extent to which information service providers may disclaim liability for loss or damage caused by service failure, or may limit their liability in those cases, is likely to vary from country to country.

2. Justification and proposed approach

22. The issues described above may affect domestic and international electronic commerce in many ways. Lack of appropriate rules, guidelines or voluntary codes of conduct, or even the perception of insufficient legal protection, undermine confidence in electronic commerce and constitute an obstacle to its development. Conflicting standards across borders may also affect the offer of goods and services,

as business entities operating under a less developed or excessively tolerant framework may enjoy an unfair competitive advantage, as compared to companies required to comply with more stringent requirements. In some cases, operations under a more lenient legal framework may be favoured by business entities interested in shielding themselves from liability that may arise under more stringent regimes. The interest of attracting investment by these companies may need to be weighed against the risk that the host country might be perceived as a safe harbour for unfair business practices, which may damage the reputation of an entire business sector.

23. The issues described above, or aspects thereof, have been under consideration by a number of international organizations, including ITU (A/CN.9/579, paras. 13-15; A/CN.9/598, paras. 24-26); OECD (see A/CN.9/579, paras. 43-51), the European Union (A/CN.9/579, paras. 32-36); APEC (A/CN.9/579, paras. 22-26; A/CN.9/598, paras. 15-17), the Commonwealth secretariat (A/CN.9/579, para. 27; A/CN.9/598, paras. 18-20) and the ICC (A/CN.9/579, paras. 53-56). Not all organizations deal with every aspect of these issues and the perspective from which each organization discusses them is not necessarily identical. This variety of sources and diversity of approaches does not facilitate the task of legislators and policy makers interested in establishing a sound legal framework for the provision of information services.

24. The Commission may wish to consider that it would be useful to include the issues of liability and standards of conduct for information service providers in a comprehensive reference document.

C. Electronic invoicing and legal issues related to supply chains in electronic commerce

1. The issues

25. It is now widely recognized that replacing trade and transport-related paper documents with electronic communications may generate significant savings and efficiency gains in international trade. Electronic equivalents of paper-based invoices play a key role in this process. If the invoices received by a buyer can be processed electronically, there will be efficiencies in working-capital management. This is especially true for geographically dispersed operations, which may need some time just to move paper documents from one place to another, but often it is true even for businesses with a single location. For instance, both buyer and supplier may benefit if the buyer is able to take advantage of discounts for early payment, which becomes much more likely when the presentment and payment cycle is reduced by weeks, perhaps to a single day or "real time".

26. However, the cost savings and efficiency gains from electronic invoicing depend to some extent on uniformity. Since the mid-1990s, many suppliers have established their own, separate systems, allowing their customers to review invoices on line; this is uniform for the supplier, but not for the buyer. A buyer may be willing to invest the necessary resources to conform to a major supplier's electronic invoices system, but is likely to find implementation of several incompatible systems of several suppliers daunting, and may resist even price incentives to be transformed from the selective customer of multiple suppliers into the hostage of one.

27. Some improvement in uniformity for buyers may be achieved by a company—frequently either a bank or a member of a corporate group—that acts as consolidator for several suppliers, although usually it is not this advantage that is emphasized, but rather the usual outsourcing benefits of cost savings, reduced capital commitment or improved efficiency for the suppliers. Some corporate groups are able to consolidate the invoices of their subsidiaries, perhaps in multiple currencies, on a netting basis, and then provide each buyer a single invoice in a single currency, again radically reducing the need for working capital. Further, banks that provide financing against invoices are able to do so more efficiently as uniformity is increased. Plainly, the greatest efficiencies for suppliers, buyers and banks would result from uniform systems across large areas, but market forces may favour uniformity less strongly than such barriers as national borders and regulations disfavour it.

28. Government involvement in electronic invoicing standards may advance related areas of electronic commerce law, such as retention of records and electronic signatures: if invoices recognized for tax purposes are electronic, then electronic record retention must be addressed, and if those invoices must be signed or stamped by the supplier, then electronic signatures or other electronic authentication must be addressed. States have established very different requirements that have made it difficult for uniform approaches to electronic invoicing that have the potential for significant cost savings to be adopted by businesses even in a single industry. These included the potential for electronic invoices to be rejected by national tax agencies, as well as concerns about cross-border recognition of electronic signatures, to the extent that they are required for the validity of an electronic invoice. Indeed, several countries that have introduced legislation to enable electronic invoicing have either expressly mandated that electronic invoices be signed electronically—sometimes even prescribing the type of signature to be used—or indirectly required the use of an authentication method by subjecting electronic invoices to a minimum level of control over the authenticity and integrity of the invoice data.

2. Justification and proposed approach

29. The introduction of electronic invoices and related aspects of electronic supply chains poses a number of technical and business management challenges. From a legal point of view, however, it seems that there are mainly two orders of possible problems: (a) how to ensure the authenticity and integrity of the electronic invoice; and (b) how to meet record-retention requirements. These issues are not novel to UNCITRAL, as they were dealt with in the provisions on electronic signatures and electronic equivalents of "original" documents and retention of electronic records in the UNCITRAL Model Law on Electronic Commerce (articles 8 and 10,

respectively). The conditions for functional equivalence between electronic records and paper-based "original" documents have more recently been spelled out in article 9, paragraphs 4 and 5, of the United Nations Convention on the Use of Electronic Communications in International Contracts. Nevertheless, a satisfactory solution to these issues, in an international context, would require, inter alia, a functioning system of cross-border recognition of electronic authentication methods.

30. A number of organizations have been working towards the formulation of standards for electronic invoicing and the development of electronic supply chains or related matters, in particular the UNECE (A/CN.9/598, paras. 31-32); WCO (A/CN.9/579, para. 52) and the European Union (A/CN.9/579, para. 38). Despite these efforts, it appears that the legal obstacles to the introduction of paperless supply chains at international scale would persist as long as the basic principles of the UNCITRAL Model Law on Electronic Commerce have not been universally implemented.

31. The Commission may wish to consider that it would be useful to include the issues of electronic invoices and electronic supply chains as part of its consideration of legal issues related to authentication and cross-border recognition of electronic signatures in a comprehensive reference document.

D. Transfer of rights in tangible goods and other rights through electronic communications

1. The issues

32. Developing electronic equivalents of traditional, mainly paper-based, methods for transferring or creating rights in tangible goods or other rights may face serious obstacles where the law requires physical delivery of goods or of paper documents for the purpose of transferring property or perfecting security interests in such goods or in the rights represented by the document. The particular problem presented by electronic commerce is how to provide a guarantee of uniqueness (or singularity) equivalent to possession of a document of title or negotiable instrument. Techniques such as those based on a combination of time-stamping and other security techniques have come close to providing a technical solution to the problem of singularity. But until an entirely satisfactory solution has been found, electronic equivalents of paper-based negotiability may have to rely on "central registry" systems, in which a central entity manages the transfer of title from one party to the next

33. Legal obstacles arising from the existence of writing and signature requirements and the probative effect of electronic communications have already been settled in articles 5 to 10 of the UNCITRAL Model Law on Electronic Commerce. Matters pertaining to contract formation in an electronic environment are settled in articles 11 to 15 of the Model Law. Also, issues related to the use of electronic means of identification to meet signature requirements have been addressed in article 7 of the UNCITRAL Model Law on Electronic Commerce and are further dealt with in the draft UNCITRAL Model Law on Electronic Signatures. More recently, "writing", "signature" and "original" requirements were addressed in article 9 of the United Nations Convention on the Use of Electronic Communications in International Contracts

34. More significant seems to be the difficulty in establishing the functional equivalence between the transfer or creation method in a paper-based environment and its electronic analogous. Where the law requires physical delivery of goods for the purpose of transferring property or perfecting security interests in such goods, a mere exchange of electronic messages between the parties would not be sufficient for effectively transferring property or perfecting security interest, however evident the parties' intention to transfer the property or perfect the security interest might have been. Therefore, even in jurisdictions where the law recognizes the legal value and effectiveness of electronic messages or records, no such message or record could alone effectively transfer property or perfect a security interest without an amendment of the law governing transfer of property or perfection of security interests.

35. The prospects for developing electronic equivalents of acts of transfer or perfection might be more positive where the law has at least in part dispensed with the strict requirement of physical delivery, for instance, by attributing to certain symbolic acts the same effect as the physical delivery of certain goods. One such example may be where the law attributes to the transferee or secured creditor the constructive possession of the goods transferred or pledged by virtue of an act of the parties that confers on the transferee the means for claiming control over the goods. Conceivably, the law could attribute the same effect to the entry of the transfer agreement into a registry system administered by a trusted third party or to an acknowledgement sent by the party in physical possession of the goods that these are held to order of the transferee or the secured creditor.

36. As noted in earlier studies by the Secretariat,[8] surmounting the issues of writing and signature in an electronic context does not solve the issue of negotiability which has been said to be "perhaps the most challenging aspect" of implementing EDI in international trade practices.[9] Rights in goods represented by documents of title are typically conditioned by the physical possession of an original paper document (the bill of lading, warehouse receipt, or other similar document). Analyses of the legal basis for the negotiability of documents of title have indicated that "[t]here is generally no statutory means in place by which commercial parties, through the exchange of electronic messages, can validly transfer legal rights in the same manner possible with paper documents".[10] This conclusion is also essentially valid for rights represented by negotiable instruments. Moreover, "the legal regime of negotiable instruments ... is in essence based on the technique of a *tangible original paper document*, susceptible to immediate visual verification on the spot. In the present state of legislation, negotiability cannot be divorced from the physical possession of the original paper document".[11]

37. Thus, it has been said that one challenge in developing law to accommodate electronically transmitted documents of title "is to generate them in such a way that holders who claim due negotiation will feel assured that there is a document of title in existence, that it has no defects upon its face, that the signature, or some substitute therefor is genuine, that it is negotiable, and that there is a means to take control of the electronic document equivalent in law to physical possession".[12]

38. The development of electronic equivalents to documents of title and negotiable instruments would therefore require the development of systems by which transactions could actually take place using electronic means of communication. This result could be achieved through a registry system, where transactions would

be recorded and managed through a central authority, or through a technical device that ensures the singularity of the relevant data message. In the case of transactions that would have used transferable or quasi-negotiable documents to transfer rights which were intended to be exclusive, either the registry system or the technical device would need to provide a reasonable guarantee as to the singularity and the authenticity of the transmitted data.

2. Justification and proposed approach

39. The establishment of electronic equivalents to paper-based registration systems raises a number of particular problems. They include the satisfaction of legal requirements of record-keeping, the adequacy of certification and authentication methods, possible need of specific legislative authority to operate electronic registration systems, the allocation of liability for erroneous messages, communication failures, and system breakdowns; the incorporation of general terms and conditions; and the safeguarding of privacy. To some extent, most of these issues are akin to issues discussed above in connection with authentication and cross-border recognition of electronic signatures (see paras. 7-13) or with liability and standards of conduct of information service providers (see paras. 18-21) above.

40. The Organization of American States (OAS) has pursued a number of initiatives related to the transfer of rights in tangible goods in recent years that involve the potential use of electronic communications. In 2002 the OAS adopted the Inter-American Uniform Through Bill of Lading for the International Carriage of Goods by the Road (Negotiable)[13] at its 6th Inter-American Specialized Conference on Private International Law (CIDIP VI[14]), held in Washington D.C. A key objective for creating this uniform bill of lading was to unify contract law in this area so as to enhance the predictability in the legal process related to the transportation of import and export goods when the mode of transportation is by road.[15] OAS has further adopted a Model Inter-American Law on Secured Transactions,[16] including an appendix on electronic documents and signatures. Issues related to electronic equivalent of maritime transport documents are also under consideration by UNCITRAL Working Group III (Transport Law), in the context of the negotiations of a draft new instrument on the carriage of goods wholly or partly by sea. Apart from these initiatives, the issues described above do not seem to be currently considered by other international organizations.

41. The Commission may wish to consider that the above constitutes an additional reason for including the issues of authentication and cross-border recognition of electronic signatures in a comprehensive reference document.

E. Unfair competition and deceptive trade practices in electronic commerce

1. The issues

42. Another policy concern is to limit fraudulent, misleading and unfair commercial practices in electronic commerce. Electronic communication permits new forms of advertising and marketing that may pose new threats to the interests of consumers as well as the functioning of the competition process. Unfair competition

law will protect these interests but legal evaluation of practices in conventional commerce cannot always be transferred to the digital environment.

43. Main features of electronic commerce on the Internet, such as interactivity, uniformity of format, and distribution in networks, allow for a convergence of mass communication and individualized communication, leading to constant renewal of forms of marketing and advertising. Advertising on the Net includes forms of banner advertising with remuneration calculated on the basis of page impressions or ad clicks. Other forms of advertisements include information that load between two content pages, either as small format pop-ups or full-page advertisements. Depending on the manner they are used, such techniques may raise issues of the separation of advertising from editorial parts of media, or may mislead customers and users to purchase services not originally intended. Unfair practices may also involve search engines, which have become the main service for users to cope with the enormous amount of information present on the Net, or use of hyperlinks for misappropriation or deceptive comparative advertising.

2. Justification and proposed approach

44. The issues described above may affect domestic and international electronic commerce in many ways. Lack of appropriate rules, guidelines or voluntary codes of conduct, or even the perception of insufficient legal protection, undermine confidence in electronic commerce and constitute an obstacle to its development. Conflicting standards across borders may also affect the offer of goods and services, as business entities operating under a less developed or excessively tolerant framework may enjoy an unfair competitive advantage, as compared to companies required to comply with more stringent requirements. In some cases, operations under a more lenient legal framework may be favoured by business entities interested in shielding themselves from liability that may arise under more stringent regimes. The interest of attracting investment by these companies may need to be weighed against the risk that the host country might be perceived as a safe harbour for unfair business practices, which may damage the reputation of an entire business sector.

45. The issues described above have been under consideration by a number of international organizations, including OECD,[17] the European Union (A/CN.9/579, para. 35); APEC (A/CN.9/579, para. 24; A/CN.9/598, para. 16), the Commonwealth secretariat (A/CN.9/579, para. 27; A/CN.9/598, paras. 18-20) and the ICC (A/CN.9/579, paras. 53-56). Not all organizations deal with every aspect of these issues and the perspective from which each organization discusses them is not necessarily identical. This variety of sources and diversity of approaches does not facilitate the task of legislators and policymakers interested in establishing a sound legal framework for consumer protection in electronic commerce, in particular in developing countries.

46. The Commission may wish to consider that it would be useful to include issues of unfair competition and deceptive trade practices in electronic commerce in a comprehensive reference document.

F. Privacy and data protection in electronic commerce

1. The issues

47. Data protection and privacy are concepts that have been acknowledged in most parts of the world, sometimes even on a constitutional law level. However, the level of protection as well as the legal instruments used to enforce it still vary considerably. With the advent of the computer there was a "first wave" of data protection initiatives in the seventies. With the spreading use of the Internet and the increased technical potential for collecting and transmitting data in electronic commerce, the protection of personal data has gained renewed attention. Practices like data mining or data warehousing as well as the placement of "cookies" are widely used in electronic commerce.

48. Data protection and privacy rules may serve the interests of user as well as of business but also have to be weighed against conflicting interests. The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is seen as an element possibly preventing economies from gaining all of the benefits of electronic commerce. On the other hand, regulatory systems restricting the flow of information can have adverse implications for global business and economies.

49. The key elements in the international discussion on principles of data protection are concerned with consent to data collection, adequate relation to the purpose, time limitation of storage, adequate level of protection in third countries to which transmission takes place, information and correction claims for users, and enhanced protection for sensitive data. New issues and restrictions on data protection arise from international security concerns, which have led to legislative actions directed at data retention. With a growing stock of international rules these do not only become more heterogeneous but also make it more difficult for companies to comply. As these standards consider conflicting interests the delineation of the field of application of these instruments as well as which of the interests protected will prevail in a specific case is gaining growing importance.

2. Justification

50. The issues described above may affect domestic and international electronic commerce in many ways. Lack of appropriate rules, guidelines or voluntary codes of conduct, or even the perception of insufficient legal protection, undermine confidence in electronic commerce and constitute an obstacle to its development. Conflicting standards across borders may also affect the offer of goods and services, as business entities operating under a less developed or excessively tolerant framework may enjoy an unfair competitive advantage, as compared to companies required to comply with more stringent requirements. In some cases, operations under a more lenient legal framework may be favoured by business entities interested in shielding themselves from liability that may arise under more stringent regimes. The interest of attracting investment by these companies may need to be weighed against the risk that the host country might be perceived as a safe harbour for unfair business practices, which may damage the reputation of an entire business sector.

51. The issues described above have been under consideration by a number of international organizations, including OECD,[18] the European Union (A/CN.9/579, para. 32); APEC (see A/CN.9/579, paras. 22-23; A/CN.9/598, para. 17), the Council of Europe (see A/CN.9/579, para. 30); the Commonwealth secretariat (A/CN.9/579, para. 27; A/CN.9/598, paras. 18-20) and the ICC (A/CN.9/579, paras. 53-56). Not all organizations deal with every aspect of these issues and the perspective from which each organization discusses them is not necessarily identical. This variety of sources and diversity of approaches does not facilitate the task of legislators and policymakers interested in establishing a sound legal framework for consumer protection in electronic commerce, in particular in developing countries.

52. The Commission may wish to consider that it would be useful to include the issues of privacy and data protection in electronic commerce in a comprehensive reference document.

G. Other elements for a sound legal framework for electronic commerce

1. Protection of intellectual property rights

53. Modern means of communication have had a significant impact in the way some intellectual property rights are defined and have challenged traditional enforcement mechanisms.

54. Copyright has been closely intertwined with the features of the production, reproduction, and distribution of works from the outset. Hence, the advent of a uniform digital format as well as digital networks poses a challenge for the specific characteristics of copyright as to subject matter, scope of rights, and enforcement as new technological possibilities and related innovative business models develop. All kinds of protected materials are now distributed and traded over digital networks. The first challenge for the legal framework is to adapt to new technological and economic developments. This concerns the scope of rights with respect to digital distribution as well as the extent of limitations to copyright. Also, certain kinds of information goods may obtain increased importance in a digital environment calling for increased protection. The protection of databases can be seen as an example. Digital networks pose a threat to traditional distribution channels and economic models as well as to existing systems of collective management. Finally, moral rights that were not in the focus of the earlier phases of computerization, which emphasized software protection, are now increasingly gaining importance with respect to the creation and distribution of works over the Internet.

55. Trademarks have an important function in commerce that is equally present in electronic commerce. While there is consensus that trademark law should apply to electronic commerce the same way as to traditional means of communication problems arise from the fact that the provisions of trademark law and protection of related signs are not tailored to the features of the new medium. Pertinent issues include: use of trademarks as meta tags, sale of trademarks as keywords, linking and framing. Further issues deriving more from "conventional" use of trademarks and related to the issue of cross-border communication as opposed to the territorial nature of trademark systems include the acquisition as well as infringement of trademark rights through use of signs on the Internet.

56. Another illustration of the impact of electronic commerce on the traditional system for protecting intellectual property rights concerns domain names. Domain names are a necessity of today's user-friendly information retrieval in the Internet. The economic value of a concise and characteristic domain cannot be underestimated. Due to this, many conflicts over certain Internet-domains have arisen. Patent law is another area affected by modern means of communication, with software patents playing an increasing role in electronic commerce.

57. States interested in developing an appropriate legal framework for electronic commerce would be well advised to consider carefully the intellectual property implications of the use of modern information and communication technologies. WIPO is the driving force in the international field for developing a framework for the protection of intellectual property. Due to the technical development much of the activity is now related to the digital environment. WIPO has a comprehensive working agenda on all aspects of intellectual property in electronic commerce. The organization's expertise and universal membership ensures the broad acceptability of the international standards set by WIPO.

2. Consumer protection in electronic commerce

58. Domestic rules on consumer protection are typically based on concerns about information asymmetries as well as a lack of negotiating power on the side of the consumer. While media such as the Internet offer convenient alternatives to traditional purchase methods, one of the main barriers to electronic commerce taking off has been the lack of consumer confidence due to uncertainties in the use of electronic media for contracting.

59. Information asymmetries are exacerbated in electronic commerce, as consumers lack vital information concerning the product, which the consumer cannot inspect physically. Consumers also have virtually no information concerning vendors and have little means to verify their identities and the standing of their business. Moreover, the features of the technical means used for the transaction may not be familiar to the consumer resulting in unintended communications. Also, there are fears that as the vendor provides the technical system it may be able to construe key features in its favour leaving the consumer in a weaker position in the transaction process. Legal uncertainties in cross-border transactions arise with respect to the applicable law and efficient ways to assert consumer claims.

60. The issues described above may affect domestic and international electronic commerce in many ways. Lack of appropriate rules, guidelines or voluntary codes of conduct, or even the perception of insufficient legal protection, undermine confidence in electronic commerce and constitute an obstacle to its development. Conflicting standards across borders may also affect the offer of goods and services, as business entities operating under a less developed or excessively tolerant framework may enjoy an unfair competitive advantage, as compared to companies required to comply with more stringent requirements. In some cases, operations under a more lenient legal framework may be favoured by business entities interested in shielding themselves from liability that may arise under more stringent regimes. The interest of attracting investment by these companies may need to be weighed against the risk that the host country might be perceived as a safe harbour for unfair business practices, which may damage the reputation of an entire business sector.

3. Unsolicited electronic communications (spam)

61. New technical means of communication, such as e-mail messaging, have also exacerbated the problems posed by unsolicited commercials. A number of countries have adopted legal instruments to combat spam. The first problem confronting anti-spam legislation is a definition of and delineation between legitimate commercial messaging and undesired spamming. Enforcement of legal anti-spam measures has proven problematic, due to the number of enforcement agencies and the variety of their powers, limitations on gathering information and sharing information as well as producing the necessary evidence, and limited enforceability across borders due to lack of national jurisdiction over cross-border spam and of appropriate measures for cross-border enforcement at the operational level.

4. Cybercrime

62. Use of modern information and communication technologies has provided new means for criminal, fraudulent or indecent activities, such as embezzlement of funds, slander, industrial espionage, violation of trade secrets or dissemination of child pornography. At the same time, new types of criminal conduct have emerged, such as identity theft, dissemination of computer viruses, or intentional breakdown of computer and information services. Besides their criminal character, all these activities may significantly affect international trade by causing physical loss or moral damage to individuals and business entities and by undermining business and consumer confidence in electronic commerce. The establishment of an effective legal framework for preventing and persecuting computer crime and cybercrime, for example, as provided for in the Convention on CyberCrime adopted by the Council of Europe[19] and its Protocol,[20] is therefore an essential component of domestic and international strategies to promote electronic commerce.

III. Proposed nature of future work

63. The Commission may wish to consider that it would be useful to include the issues described in Part II, sections A to F, as well as other related issues in a comprehensive reference document. The document would describe in some detail the issues discussed above and the solutions being offered or proposed by the various organizations that have worked in this area. The Secretariat proposes that the legislative guidance document should take a narrative and neutral approach to issues dealt with by other organizations and should not be intended as a comparative evaluation of the solutions proposed by them. Neither should the document offer its own advice as an alternative to or substitute for the advice of other organizations.

64. The Secretariat proposes a different approach as regards issues related to intellectual property rights, which are described in Part II, paragraphs 53-57 above, and which have been extensively treated at a universal level under the auspices of WIPO. In respect of those issues, the Commission may wish to consider that it would be worth mentioning them in any comprehensive reference document that the Commission might wish to prepare, although in a somewhat summary form, with a view to drawing the attention of legislators and policymakers to the importance of establishing an appropriate legal framework for the protection of intellectual property rights in electronic commerce.

65. As regards issues related to consumer protection, unsolicited commercial communications, cybercrime and computer crime, which are described respectively in Part II, paragraphs 64 and 65 above, the Secretariat proposes to treat those topics in a similarly abbreviated manner that would highlight their importance and refer to ongoing and completed work by the relevant organizations.

Notes

[1] *Official Records of the General Assembly, Sixtieth Session, Supplement No. 17* (A/60/17), paras 213-215.

[2] For the text of the Model Law, see *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), annex I. The Model Law and its accompanying Guide to Enactment have been published as a United Nations publication (Sales No. E.99.V.4).

[3] For the text of the Model Law, see *Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 17* (A/56/17), annex II. The Model Law and its accompanying Guide to Enactment have been published as a United Nations publication (Sales No. E.02.V.8).

[4] For the text of the Convention, see the Annex to General Assembly resolution 60/21, of 23 November 2005.

[5] *Official Records of the General Assembly, Sixtieth Session, Supplement No. 17* (A/60/17), para. 213.

[6] Ibid., para. 214.

[7] Ibid., para. 214.

[8] A/CN.9/WG.IV/WP.69 (*Yearbook of the United Nations Commission on International Trade Law* (UNCITRAL Yearbook), vol. XXVII: 1996 (Sales No.: E.98.V.7), part two, chap. II, sect. B), para. 55; A/CN.9/WG.IV/WP.90 (UNCITRAL Yearbook, vol. XXXII: 2001 (Sales No.: E.04.V.4) part two, chap. II, sect. F), para. 35.

[9] See Jeffrey B. Ritter and Judith Y. Gliniecki, "International Electronic Commerce and Administrative Law: The Need for Harmonized National Reforms", Harvard Journal of Law and Technology, vol. 6 (1993), p. 279.

[10] Ibid.

[11] See K. Bernauw, "Current developments concerning the form of bills of lading—Belgium", Ocean Bills of Lading: Traditional Forms, Substitutes and EDI Systems, A. N. Yannopoulos, editor (The Hague, Kluwer Law International, 1995), p. 114.

[12] Donald B. Pedersen, "Electronic data interchange as documents of title for fungible agricultural commodities", Idaho Law Review, vol. 31 (1995), p. 726.

[13] Inter-American Uniform Through Bill of Lading for the International Carriage of goods by the Road (Negotiable), available at http://www.oas.org/DIL/CIDIP-VI-billoflanding-Eng.htm.

[14] Conferencias Especializadas Interamericanas sobre Derecho Internacional Privado.

[15] See, "Summary" at http://www.oas.org/DIL/CIDIP-VI-billoflanding-Eng_summary.htm. Two areas of this convention deal with electronic issues. First, Article 2 defines a "Writing" as including "a written document, a telegram, telex, telephonic facsimile (fax), electronic data interchange, or a document created or transferred by electronic means" [emphasis added]. Additionally, article 18.1 of this treaty provides for the possibility of electronic signatures, as well as other signature types, if authorized by applicable law.

[16] http://www.oas.org/DIL/CIDIP-VI-securedtransactions_Eng.htm. This Model Law was approved by the Plenary meeting of delegates on 8 February 2002 as resolution CIDIP-VI/RES.5/02, which can be accessed at http://www.oas.org/main/main.asp?sLang=E&sLink= http://www.oas.org/dil/. The Model Law itself may be accessed (in Spanish and English) at http://www.oas.org/dil/Annex_cidipviRES.%205-02.pdf. (Last visited, 12 April 2006.)

[17] See the OECD, Ministerial Declaration on Consumer Protection in the Context of Electronic Commerce of 8-9 October 1998, http://www.oecd.org/LongAbstract/0,2546,en_2649_34267_1865273_119672_1_1_1,00.html (10.3.2006).

[18] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, applicable on 23 September 1980: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. See further the OECD "Privacy Policy Generator" (http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html).

[19] The CyberCrime Convention, ETS 185, entered into force on 1 July 2004. It is intended to develop a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate criminal legislation and fostering international cooperation. *Source*: Council of Europe Treaty Office, http://conventions.coe.int/.

[20] The Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature supplements, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime as regards the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189). It was opened for signature in Strasbourg on 28 January 2003. Source: Council of Europe Treaty Office, http://conventions.coe.int/.